UNITED STATES DISTRICT COURT
NORTHEN DISTRICT OF ILLINOIS
WESTERN DIVISION

DEBRA WHITLOCK, on behalf of herself and all others similarly situated, Plaintiff, v. **RRCA ACCOUNTS MANAGEMENT, INC.,** Defendant.	Case No.: _____ JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Debra Whitlock ("Plaintiff"), individually and on behalf of all similarly situated persons, allege the following against RRCA Accounts Management, Inc. ("RRCA" or "Defendant") based upon personal knowledge with respect to herself and on information and belief derived from, among other things, investigation by Plaintiff's counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiff brings this class action against RRCA for its failure to properly secure and safeguard Plaintiff's and other similarly situated RRCA customers' patients' personally identifiable information ("PII") and protected health information ("PHI"), including names, Social Security numbers, driver's license numbers, passport numbers, health insurance numbers, protected health data- such as billing and insurance claims, and payment card and account numbers (the "Private Information"), from criminal hackers.

2. RRCA, based in Sterling, Illinois, is a full-service collection agency that serves businesses along Lincoln Highway in Dekalb, Illinois and Clinton, Iowa.

3. On or about October 24, 2024, RRCA filed official notice of a hacking incident with the Office of the Attorney General of New Hampshire. Under state and federal law, organizations must report breaches involving PHI within at least sixty (60) days.

4. On or about October 18, 2024, RRCA also sent out data breach letters (the "Notice") to individuals whose information was compromised as a result of the hacking incident.

5. Based on the Notice sent to Plaintiff and "Class Members" (defined below), unusual activity was detected on some of its computer systems. In response, Defendant took action to stop the activity. RRCA's investigation revealed that an unauthorized party, using Play ransomware[1], had access to certain files that contained sensitive customer information, and that such access took place on or around June 6, 2024 (the "Data Breach"). Yet, RRCA waited ***four months*** to notify the public that they were at risk.

6. As a result of this delayed response, Plaintiff and Class Members had no idea for four months that their Private Information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

7. The Private Information compromised in the Data Breach contained highly sensitive patient data, representing a gold mine for data thieves. The data included, but is not limited to, Social Security numbers, health insurance numbers, protected health data- such as billing and insurance claims, and payment information.

[1] https://www.prnewswire.com/news-releases/rrca-accounts-management-inc-reports-ransomware-attack-and-data-breach-302280547.html (Last visited Nov. 18, 2024).

8. Armed with the Private Information accessed in the Data Breach (and a head start), data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

9. There has been no assurance offered by RRCA that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

10. Therefore, Plaintiff and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering, ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

11. Plaintiff brings this class action lawsuit to address RRCA's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and its failure to provide timely and adequate notice to Plaintiff and Class Members of the types of information that were accessed, and that such information was subject to unauthorized access by cybercriminals.

12. The potential for improper disclosure and theft of Plaintiff's and Class Members' Private Information was a known risk to RRCA, and thus RRCA was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

13. Upon information and belief, RRCA failed to properly monitor and properly implement security practices with regard to the computer network and systems that housed the Private Information. Had RRCA properly monitored its networks, it would have discovered the Breach sooner.

14. Plaintiff's and Class Members' identities are now at risk because of RRCA's negligent conduct as the Private Information that RRCA collected and maintained is now in the hands of data thieves and other unauthorized third parties.

15. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

16. Accordingly, Plaintiff, on behalf of herself and the Class, assert claims for negligence, negligence *per se*, breach of third party beneficiary contract, violation of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/2, *et seq*, unjust enrichment, and declaratory judgment.

II. PARTIES

17. Plaintiff Debra Whitlock is, and at all times mentioned herein was, an individual citizen of the State of Illinois.

18. Defendant RRCA is a collection service company incorporated in Illinois with its principal place of business at 201 East 3rd Street, Sterling, IL 61081 in Whiteside County.

III. JURISDICTION AND VENUE

19. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from RRCA. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

20. This Court has jurisdiction over RRCA because RRCA operates in and/or is incorporated in this District.

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and RRCA has harmed Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

A. RRCA's Business and Collection of Plaintiff's and Class Members' Private Information

22. RRCA is a full-service collection agency, founded in 1979. Although medical care facilities and providers are its primary market, RRCA services utility and retail clients, all sizes of businesses, property owners, and municipalities. RRCA employs more than 25 people and generates approximately $5 million in annual revenue.

23. As a condition of receiving collection services, RRCA requires that its customers entrust it with their patients' highly sensitive personal and health information. In the ordinary course of receiving service from RRCA, Plaintiff and Class Members healthcare providers were required to provide their patients' Private Information to Defendant.

24. Due to the highly sensitive and personal nature of the information RRCA acquires and stores with respect to its customers' patients, RRCA, upon information and belief, promises

to, among other things: keep customers' patients' Private Information private; comply with industry standards related to data security and the maintenance of its customers' patients' Private Information; inform its customers' patients of its legal duties relating to data security and comply with all federal and state laws protecting customers' patients' Private Information; only use and release customers' patients' Private Information for reasons that relate to the services it provides; and provide adequate notice to customers' patients if their Private Information is disclosed without authorization.

25. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, RRCA assumed legal and equitable duties it owed to them and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure and exfiltration.

26. Plaintiff and Class Members healthcare providers relied on RRCA to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendant ultimately failed to do.

B. The Data Breach and Defendant's Inadequate Notice to Plaintiff and Class Members

27. According to Defendant's Notice, it learned of unauthorized access to its computer systems on August 20, 2024, with such unauthorized access having taken place on or around June 6, 2024.

28. Through the Data Breach, the unauthorized cybercriminal(s) with Play accessed a cache of highly sensitive Private Information, including names, Social Security numbers, driver's license numbers, passport numbers, health insurance numbers, protected health data- such as billing and insurance claims, and payment card and account numbers.

29. Play, which also goes by the names "Balloonfly", "Fiddling Scorpius", and "PlayCrypt", is a notorious ransomware group that is believed to have impacted "approximately 300 organizations as of October 2023", and recently has reportedly begun collaborating with North Korean threat actors.[2]

30. On or about October 18, 2024, roughly four (4) months after RRCA learned that the Class's Private Information was first accessed by cybercriminals, RRCA finally began to notify customers' patients that its investigation determined that their Private Information was accessed.

31. RRCA delivered Data Breach Notification Letters to Plaintiff and Class Members, alerting them that their highly sensitive Private Information had been exposed in a "security incident."

32. Omitted from the Notice are crucial details like the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information is protected.

33. Thus, RRCA's purported disclosure amounts to no real disclosure at all, as it fails to inform Plaintiff and Class Members of the Data Breach's critical facts with any degree of specificity. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach was and is severely diminished.

34. RRCA had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

[2] Ravie Lakshmanan, *North Korean Group Collaborates with Play Ransomware in Significant Cyber Attack*, (October 30, 2024), https://thehackernews.com/2024/10/north-korean-group-collaborates-with.html (Last visited Nov. 18, 2024).

35. Plaintiff and Class Members provided their Private Information to RRCA with the reasonable expectation and mutual understanding that RRCA would comply with its obligations to keep such Information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

36. RRCA's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

37. RRCA knew or should have known that its electronic records would be targeted by cybercriminals.

C. The Healthcare Sector is Particularly Susceptible to Data Breaches

38. RRCA was on notice that companies in and around the healthcare industry are susceptible targets for data breaches.

39. In August 2014, after a cyberattack on Community Health Systems, Inc., the Federal Bureau of Investigation ("FBI") warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PHI)."[3]

40. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of

[3] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), *available at* https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited on Nov. 18, 2024).

> patients' health and financial information, but also patient access to care.[4]

41. The healthcare sector reported the second largest number of data breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[5] In 2022, the largest growth in compromises occurred in the healthcare sector.[6]

42. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident … came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[7]

43. Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[8]

---

[4] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n. (Oct. 4, 2019), *available at*: https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited on Nov. 18, 2024).

[5] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report, available at*: https://www.idtheftcenter.org/wp-content/uploads/2019/01/ITRC_2018-EOY-BREACH-REPORT-KEY-FINDINGS.pdf (last visited on Nov. 18, 2024).

[6] Identity Theft Resource Center, *2022 End-of-Year Data Breach Report, available at*: https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf (last visited on Nov. 18, 2024).

[7] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/ (last visited on Nov. 18, 2024).

[8] *Id*.

44. Healthcare related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[9]

45. As a healthcare provider, RRCA knew, or should have known, the importance of safeguarding its customers' patients' Private Information, including PHI, entrusted to it, and of the foreseeable consequences if such data were to be disclosed. These consequences include the significant costs that would be imposed on RRCA's customers' patients as a result of a breach. RRCA failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

D. RRCA Failed to Comply with HIPAA

46. Title II of HIPAA contains what are known as the Administration Simplification provisions. *See* 42 U.S.C. §§ 1301, *et seq*. These provisions require that HHS create rules to streamline the standards for handling PHI similar to the data Defendant left unguarded and vulnerable to attack. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

47. RRCA's Data Breach resulted from a combination of insufficiencies that indicate RRCA failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from RRCA's Data Breach that RRCA either failed to implement, or

[9] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last visited on Nov. 18, 2024).

inadequately implemented, information security policies or procedures to protect Plaintiff's and Class Members' PHI.

48. Plaintiff's and Class Members' Private Information compromised in the Data Breach included "protected health information" as defined by CFR § 160.103.

49. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

50. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

51. Plaintiff's and Class Members' Private Information included "unsecured protected health information" as defined by 45 CFR § 164.402.

52. Plaintiff's and Class Members' unsecured PHI was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

53. Based upon Defendant's Notice to Plaintiff and Class Members, RRCA reasonably believes that Plaintiff's and Class Members' unsecured PHI has been acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

54. Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

55. RRCA reasonably believes that Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart

E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

56. Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

57. Plaintiff's and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

58. RRCA reasonably believes that Plaintiff's and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

59. It is reasonable to infer that Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

60. It should be rebuttably presumed that unsecured PHI acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

61. After receiving notice that they were victims of the Data Breach (which required the filing of a data breach report in accordance with 45 CFR § 164.408(a)), it is reasonable for recipients of that notice, including Plaintiff and Class Members in this case, to believe that future

harm (including medical identity theft) is real and imminent, and to take steps necessary to mitigate that risk of future harm.

62. In addition, RRCA's Data Breach could have been prevented if RRCA had implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PHI when it was no longer necessary and/or had honored its obligations to its customers' patients.

63. RRCA's security failures also include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information RRCA creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents;

g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);

h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);

i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3);

j. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce, in violation of 45 CFR 164.306(a)(94); and

k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

64. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414 also required RRCA to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***" (emphasis added).

65. Because RRCA has failed to comply with HIPAA, while monetary relief may cure some of Plaintiff's and Class Members' injuries, injunctive relief is also necessary to ensure RRCA's approach to information security is adequate and appropriate going forward. RRCA still maintains the PHI and other highly sensitive PII of its current and former customers' patients, including Plaintiff and Class Members. Without the supervision of the Court through injunctive relief, Plaintiff's and Class Members' Private Information remains at risk of subsequent data breaches.

E. RRCA Failed to Comply with FTC Guidelines

66. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

67. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[10] . The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

68. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for

[10] *Protecting Personal Information: A Guide for Business,* FEDERAL TRADE COMMISSION (October 2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited on Nov. 18, 2024).

suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

69. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45 *et seq*. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

70. Such FTC enforcement actions include those against businesses that fail to adequately protect customer data, like RRCA here. *See, e.g.*, *In the Matter of LabMD, Inc*., 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

71. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like RRCA of failing to use reasonable measures to protect Private Information they collect and maintain from consumers. The FTC publications and orders described above also form part of the basis of RRCA's duty in this regard.

72. The FTC has also recognized that personal data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The

larger the data set, the greater potential for analysis and profit."[11]

73. As evidenced by the Data Breach, RRCA failed to properly implement basic data security practices. RRCA's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

74. RRCA was at all times fully aware of its obligation to protect the Private Information of its customers' patients yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

F. RRCA Failed to Comply with Industry Standards

75. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

76. The Center for Internet Security's (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security,

[11] FTC Commissioner Pamela Jones Harbour, *Remarks Before FTC Exploring Privacy Roundtable* (Dec. 7, 2009), *transcript available at* https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf (last visited on Nov. 18, 2024).

Incident Response Management, and Penetration Testing.[12]

77. The National Institute of Standards and Technology ("NIST") also recommends certain practices to safeguard systems, such as the following:

a. Control who logs on to your network and uses your computers and other devices.
b. Use security software to protect data.
c. Encrypt sensitive data, at rest and in transit.
d. Conduct regular backups of data.
e. Update security software regularly, automating those updates if possible.
f. Have formal policies for safely disposing of electronic files and old devices.
g. Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

78. Further still, the United States Cybersecurity and Infrastructure Security Agency ("CISA") makes specific recommendations to organizations to guard against cybersecurity attacks, including (a) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps; (b) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that

[12] *The 18 CIS Critical Security Controls*, CENTER FOR INTERNET SECURITY, https://www.cisecurity.org/controls/cis-controls-list (last visited on Nov. 18, 2024).

signatures in these tools are updated," and (c) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.[13]

79. Defendant failed to implement industry-standard cybersecurity measures, including by failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and by failing to comply with other industry standards for protecting Plaintiff's and Class Members' Private Information, resulting in the Data Breach.

G. RRCA Breached its Duty to Safeguard Plaintiff's and Class Members' Private Information

80. In addition to its obligations under federal and state laws, RRCA owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. RRCA owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

81. RRCA breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer

[13] *Shields Up: Guidance for Organizations*, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, https://www.cisa.gov/shields-guidance-organizations (last visited Nov. 18, 2024).

systems and data. RRCA's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect customers' patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees regarding the proper handling of its customers' patients' Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to HIPAA and industry standards for cybersecurity as discussed above; and

g. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

82. RRCA negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

83. Had RRCA remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential Private Information.

84. Accordingly, Plaintiff's and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of

future harm that includes, but is not limited to, fraud and identity theft. Plaintiff and Class Members also lost the benefit of the bargain they made with RRCA.

H. Plaintiff and Class Members are at a Significantly Increased and Substantial Risk of Fraud and Identity Theft as a Result of the Data Breach.

85. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiff and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[14] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

86. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

87. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security

[14] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on Nov. 18, 2024).

number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

88. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

89. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiff and Class Members.

90. One such example of how malicious actors may compile Private Information is through the development of "Fullz" packages.

91. ""Cybercriminals can cross-reference two sources of the Private Information compromised in the Data Breach to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

92. The development of "Fullz" packages means that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card or financial account numbers

may not be included in the Private Information stolen in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other Class Members' stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

93. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[15] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

94. Identity thieves can also use stolen personal information such as Social Security numbers and PHI for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

[15] *See IdentityTheft.gov,* Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited Nov. 18, 2024).

95. The Identity Theft Resource Center documents the multitude of harms caused by fraudulent use of PII in its 2023 Consumer Impact Report.[16] After interviewing over 14,000 identity crime victims, researchers found that as a result of the criminal misuse of their PII:

- 77-percent experienced financial-related problems;
- 29-percent experienced financial losses exceeding $10,000;
- 40-percent were unable to pay bills;
- 28-percent were turned down for credit or loans;
- 37-percent became indebted;
- 87-percent experienced feelings of anxiety;
- 67-percent experienced difficulty sleeping; and
- 51-percent suffered from panic of anxiety attacks.[17]

96. PHI is also especially valuable to identity thieves. As the FTC recognizes, identity thieves can use PHI to commit an array of crimes, including identity theft and medical and financial fraud.[18]

97. Indeed, a robust cyber black market exists in which criminals openly post stolen PHI on multiple underground Internet websites, commonly referred to as the dark web.

98. While credit card information and associated PII can sell for as little as $1-$2 on the black market, protected health information can sell for as much as $363 according to the Infosec Institute.[19]

---

[16] *2023 Consumer Impact Report* (Jan. 2024), IDENTITY THEFT RESOURCE CENTER, *available online at*: https://www.idtheftcenter.org/wp-content/uploads/2023/08/ITRC_2023-Consumer-Impact-Report_Final-1.pdf (last visited on Nov. 18, 2024).

[17] *Id* at pp 21-25.

[18] Federal Trade Commission, *Warning Signs of Identity Theft, available at*: https://consumer.ftc.gov/articles/what-know-about-identity-theft (last visited on Nov. 18, 2024).

[19] *Data Breaches: In the Healthcare Sector,* CENTER FOR INTERNET SECURITY, *available at*: https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited on Nov. 18, 2024).

99. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

100. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[20]

101. The ramifications of RRCA's failure to keep its customers' patients' Private Information secure are long lasting and severe. Once it is stolen, fraudulent use of such and damage to victims may continue for years.

102. Here, not only was sensitive medical information compromised, but financial information and Social Security numbers were compromised too. The value of both PII and PHI is axiomatic. The value of "big data" in corporate America is astronomical. The fact that identity thieves attempt to steal identities notwithstanding possible heavy prison sentences illustrates beyond a doubt that the Private Information compromised here has considerable market value.

103. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or PHI is stolen and when it is

[20] Michael Ollove, "*The Rise of Medical Identity Theft in Healthcare*," KAISER HEALTH NEWS (Feb. 7, 2014), *available at*: https://kffhealthnews.org/news/rise-of-indentity-theft/ (last visited on Nov. 18, 2024).

misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[21]

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

104. PII and PHI are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years.

105. As a result, Plaintiff and Class Members are at an increased risk of fraud and identity theft, including medical identity theft, for many years into the future. Thus, Plaintiff and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

I. Plaintiff's and Class Members' Damages

Plaintiff Whitlock's Experience

106. Plaintiff Whitlock is a patient of CGH Medical Center, a customer of Defendant who had her Private Information provided to Defendant as a condition of receiving collection agency services on behalf of CGH Medical Center.

107. When CGH Medical Center became a customer, Defendant required CGH Medical Center provide it with substantial amounts of Plaintiff Whitlock's Private Information, including PHI.

[21] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, U.S. GOVERNMENT ACCOUNTABILITY OFFICE (June 2007), *available at* https://www.gao.gov/assets/gao-07-737.pdf (last visited on Nov. 18, 2024).

108. On or about October 18, 2024, Plaintiff Whitlock received the Notice, which told her that her Private Information had been accessed during the Data Breach. The Notice informed her that the Private Information stolen may have included her "Social Security number, driver's license number, passport number, telephone number, health insurance information, health data, such as medical record numbers and places of treatments and doctors, health payment information, username or IP address, and demographic information".

109. Plaintiff Whitlock suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring her accounts for fraud.

110. Plaintiff Whitlock would not have provided her Private Information to CGH Medical Center or Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices to safeguard its customers' patients' personal and health information from theft, and that those systems were subject to a data breach.

111. Plaintiff Whitlock suffered actual injury in the form of having her PII and PHI compromised and/or stolen as a result of the Data Breach.

112. Plaintiff Whitlock suffered actual injury in the form of damages to and diminution in the value of her personal, health, and financial information – a form of intangible property that CGH Medical Center entrusted to Defendant for the purpose of receiving collection services from Defendant and which was compromised in, and as a result of, the Data Breach.

113. Plaintiff Whitlock suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by her Private Information being placed in the hands of criminals.

114. Plaintiff Whitlock has a continuing interest in ensuring that her Private Information, which remains in the possession of Defendant, is protected and safeguarded from future breaches. This interest is particularly acute, as Defendant's systems have already been shown to be susceptible to compromise and are subject to further attack so long as RRCA fails to undertake the necessary and appropriate security and training measures to protect its customers' patients' Private Information

115. As a result of the Data Breach, Plaintiff Whitlock made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant. Plaintiff has spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

116. As a result of the Data Breach, Plaintiff Whitlock has suffered anxiety as a result of the release of her PII and PHI, which she believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using her PII and PHI for purposes of committing cyber and other crimes against her including, but not limited to, fraud and identity theft. Plaintiff is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach would have on her life.

117. Plaintiff Whitlock also suffered actual injury from having her Private Information compromised as a result of the Data Breach in the form of (a) damage to and diminution in the value of her PII and PHI, a form of property that Defendant obtained from CGH Medical Center and Plaintiff; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud she now faces.

118. As a result of the Data Breach, Plaintiff Whitlock anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

119. In sum, Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

120. Plaintiff and Class Members healthcare providers entrusted their Private Information to Defendant in order to receive Defendant's services.

121. Their Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendant's inadequate data security practices.

122. As a direct and proximate result of RRCA's actions and omissions, Plaintiff and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having medical services billed in their names, loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

123. Further, and as set forth above, as a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

124. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

125. Plaintiff and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiff and Class Members.

126. The Private Information maintained by and stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiff and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiff and Class Members.

127. Plaintiff and Class Members also lost the benefit of the bargain they made with RRCA. Plaintiff and Class Members overpaid for services that were intended to be accompanied by adequate data security but were not. Indeed, part of the price Plaintiff and Class Members paid to RRCA was intended to be used by RRCA to fund adequate security of RRCA's system and protect Plaintiff's and Class Members' Private Information. Thus, Plaintiff and the Class did not receive the benefit of the bargain.

128. Additionally, Plaintiff and Class Members also suffered a loss of value of their PII and PHI when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth

roughly $200 billion.[22] In fact, consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[23]

129. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiff and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiff and the Class Members, thereby causing additional loss of value.

130. Finally, Plaintiff and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

131. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of RRCA, is protected from future breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing highly sensitive personal and health information of its customers' patients are not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

---

[22] *See How Data Brokers Profit from the Data We Create*, THE QUANTUM RECORD, https://thequantumrecord.com/blog/data-brokers-profit-from-our-data/ (last visited on Nov. 18, 2024).

[23] *Frequently Asked Questions,* NIELSEN COMPUTER & MOBILE PANEL, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited on Nov. 18, 2024).

132. As a direct and proximate result of RRCA's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

133. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

134. Specifically, Plaintiff proposes the following Nationwide Class (referred to herein as the "Class"), subject to amendment as appropriate:

> **Nationwide Class**
>
> All individuals in the United States who had Private Information accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

135. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

136. Plaintiff reserves the right to modify or amend the definitions of the proposed Nationwide Class, as well as the addition of any subclasses before the Court determines whether certification is appropriate.

137. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

138. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of all patients of customers of RRCA whose

data was compromised in the Data Breach. The identities of Class Members are ascertainable through RRCA's records, Class Members' records, publication notice, self-identification, and other means.

139. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether RRCA engaged in the conduct alleged herein;

b. Whether RRCA's conduct violated the FTCA and/or HIPAA;

c. When RRCA learned of the Data Breach

d. Whether RRCA's response to the Data Breach was adequate;

e. Whether RRCA unlawfully lost or disclosed Plaintiff's and Class Members' Private Information;

f. Whether RRCA failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

g. Whether RRCA's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

h. Whether RRCA's data security systems prior to and during the Data Breach were consistent with industry standards;

i. Whether RRCA owed a duty to Class Members to safeguard their Private Information;

j. Whether RRCA breached its duty to Class Members to safeguard their Private Information;

k. Whether hackers obtained Class Members' Private Information via the Data Breach;

l. Whether RRCA had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;

m. Whether RRCA breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

n. Whether RRCA knew or should have known that its data security systems and monitoring processes were deficient;

o. What damages Plaintiff and Class Members suffered as a result of RRCA's misconduct;

p. Whether RRCA's conduct was negligent;

q. Whether RRCA's conduct was *per se* negligent;

r. Whether RRCA was unjustly enriched;

s. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;

t. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

u. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

140. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*,

all Class Members were injured through the common misconduct of RRCA. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

141. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

142. Predominance. RRCA has engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from RRCA's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

143. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for RRCA. In contrast, conducting this action as a class action presents far fewer management difficulties,

conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

144. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). RRCA has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

145. Finally, all members of the proposed Class are readily ascertainable. RRCA has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by RRCA.

CLAIMS FOR RELIEF
COUNT I
NEGLIGENCE
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

146. Plaintiff restates and realleges all of the allegations stated above as if fully set forth herein.

147. RRCA knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

148. RRCA's duty also included a responsibility to implement processes by which it could detect and analyze a breach of its security systems quickly and to give prompt notice to those affected in the case of a cyberattack.

149. RRCA knew or should have known of the risks inherent in collecting the Private Information of Plaintiff and Class Members and the importance of adequate security. RRCA was

on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

150. RRCA owed a duty of care to Plaintiff and Class Members whose Private Information was entrusted to it. RRCA's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect customers' patients' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class Members pursuant to HIPAA and the FTCA;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiff and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

151. RRCA's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

152. RRCA's duty also arose because Defendant was bound by industry standards to protect its customers' patients' confidential Private Information.

153. Plaintiff and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and RRCA owed them a duty of care to not subject them to an unreasonable risk of harm.

154. RRCA, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within RRCA's possession.

155. RRCA, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiff and Class Members.

156. RRCA, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

157. RRCA breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to comply with the FTCA;

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

158. RRCA acted with reckless disregard for the rights of Plaintiff and Class Members by failing to provide prompt and adequate individual notice of the Data Breach such that Plaintiff and Class Members could take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

159. RRCA had a special relationship with Plaintiff and Class Members. Plaintiff's and Class Members' willingness to entrust RRCA with their Private Information was predicated on the understanding that RRCA would take adequate security precautions. Moreover, only RRCA had the ability to protect its systems (and the Private Information that it stored on them) from attack.

160. RRCA's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised and exfiltrated, as alleged herein.

161. As a result of RRCA's ongoing failure to notify Plaintiff and Class Members regarding exactly what Private Information has been compromised, Plaintiff and Class Members have been unable to take the necessary precautions to prevent future fraud and mitigate damages.

162. RRCA's breaches of duty also caused a substantial, imminent risk to Plaintiff and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

163. As a result of RRCA's negligence in breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

164. RRCA also had independent duties under state laws that required it to reasonably safeguard Plaintiff's and Class Members' Private Information and promptly notify them about the Data Breach.

165. As a direct and proximate result of RRCA's negligent conduct, Plaintiff and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

166. The injury and harm that Plaintiff and Class Members suffered was reasonably foreseeable.

167. Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

168. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring RRCA to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT II
NEGLIGENCE *PER SE*
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

169. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

170. Pursuant to Section 5 of the FTCA, RRCA had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiff and Class Members.

171. Pursuant to HIPAA, 42 U.S.C. § 1302(d), *et seq*., RRCA had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Private Information.

172. Specifically, pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key." *See* definition of "encryption" at 45 C.F.R. § 164.304.

173. RRCA breached its duties to Plaintiff and Class Members under the FTCA and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

174. Specifically, RRCA breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

175. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII and PHI (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of RRCA's duty in this regard.

176. RRCA also violated the FTCA and HIPAA by failing to use reasonable measures to protect the Private Information of Plaintiff and the Class and by not complying with applicable industry standards, as described herein.

177. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiff's and Class Members' Private Information in compliance with applicable laws would result in an

unauthorized third-party gaining access to RRCA's networks, databases, and computers that stored Plaintiff's and Class Members' unencrypted Private Information.

178. Plaintiff and Class Members are within the class of persons that the FTCA and HIPAA are intended to protect and RRCA's failure to comply with both constitutes negligence *per se*.

179. Plaintiff's and Class Members' Private Information constitutes personal property that was stolen due to RRCA's negligence, resulting in harm, injury, and damages to Plaintiff and Class Members.

180. As a direct and proximate result of RRCA's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to damages from the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

181. As a direct and proximate result of RRCA's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

182. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring RRCA to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT III
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

183. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

184. Defendant entered into contracts, written or implied, with its healthcare entity clients to perform services that include, but are not limited to, providing payment collection services. Upon information and belief, these contracts are virtually identical between and among Defendant and its clients around the country whose patients, including Plaintiff and Class Members, were affected by the Data Breach.

185. In exchange, Defendant agreed, in part, to implement adequate security measures to safeguard the Private Information of Plaintiff and the Class.

186. These contracts were made expressly for the benefit of Plaintiff and the Class, as Plaintiff and Class Members were the intended third-party beneficiaries of the contracts entered into between Defendant and its clients. Defendant knew that if it were to breach these contracts with its clients, the clients' patients—Plaintiff and Class Members—would be harmed.

187. Defendant breached the contracts it entered into with its clients by, among other things, failing to (i) use reasonable data security measures, (ii) implement adequate protocols and employee training sufficient to protect Plaintiff's Private Information from unauthorized disclosure to third parties, and (iii) promptly and adequately detecting the Data Breach and notifying Plaintiff and Class Members thereof.

188. Plaintiff and the Class were harmed by Defendant's breach of its contracts with its clients, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

189. Plaintiff and Class Members are also entitled to their costs and attorney's fees incurred in this action.

COUNT IV
VIOLATION OF ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT, 815 ILCS 505/2, *et seq.*
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

190. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

191. Defendant engaged in unlawful and unfair practices in violation of the ICFA by failing to maintain reasonable security measures to protect and secure Plaintiff and Class Members' Private Information in a manner that complied with applicable laws, regulations, and industry standards.

192. Defendant's duties also arise from the Illinois Private Information Protection Act, 815 ILCS 530/45(a) which requires: "A data collector that owns or licenses or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure."

193. Defendant violated this duty by failing to, or contracting with companies that failed to, implement reasonably secure data security policies.

194. Due to the Data Breach, Plaintiff and Class Members have lost property in the form of their Private Information. This breach will force Plaintiff and Class Members to spend time or money to protect against identity theft. Plaintiff and Class Members are now at a higher risk of medical identity theft and other crimes for the remainder of their lifetimes. This harm sufficiently outweighs any justifications or motives for Defendant's practice of collecting and storing Private Information without appropriate and reasonable safeguards to protect such information.

195. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have been harmed and have suffered damages including, but not limited to: (i) invasion

of privacy; (ii) theft of their Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

196. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices alleged herein, Plaintiff and Class members have been damaged and are entitled to recover an order providing declaratory and injunctive relief and reasonable attorneys' fees and costs, to the extent permitted by law.

COUNT V
UNJUST ENRICHMENT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

197. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

198. This Count is pleaded in the alternative to Counts III above.

199. Plaintiff and Class Members conferred a benefit on RRCA by permitting their healthcare providers – Defendant's clients – to turn over their inherently valuable Private Information to Defendant.

200. Defendant, in turn, enriched itself by saving the costs it should have expended on data security measures to secure Plaintiff's and Class Members' Private Information.

201. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

202. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

203. Defendant acquired the monetary benefit and Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

204. If Plaintiff and Class Members knew that Defendant had not secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

205. Plaintiff and Class Members have no adequate remedy at law.

206. Due to RRCA's conduct alleged herein, it would be unjust and inequitable under the circumstances for RRCA to be permitted to retain the benefit of its wrongful conduct.

207. As a direct and proximate result of RRCA's conduct, Plaintiff and Class Members have suffered, and/or are at a continued, imminent risk of suffering, injury that includes but is not limited to the following: (i) the loss of the opportunity to control how their Private Information is used; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future

consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in RRCA's possession and is subject to further unauthorized disclosures so long as RRCA fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

208. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from RRCA and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by RRCA from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

209. Plaintiff and Class Members may not have an adequate remedy at law against RRCA, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT VI
DECLARATORY JUDGMENT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

210. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

211. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious

and violate the terms of the federal laws and regulations and state statute described in this Complaint.

212. RRCA owes a duty of care to Plaintiff and Class Members, which required it to adequately secure Plaintiff's and Class Members' Private Information.

213. RRCA still possesses Private Information regarding Plaintiff and Class Members.

214. Plaintiff alleges that RRCA's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of her Private Information and the risk remains that further compromise of her Private Information will occur in the future.

215. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. RRCA owes a legal duty to secure its customers' patients' Private Information and to timely notify customers' patients of a data breach under the common law, HIPAA, and the FTCA;

b. RRCA's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect customers' patients' Private Information; and

c. RRCA continues to breach this legal duty by failing to employ reasonable measures to secure customers' patients' Private Information.

216. This Court should also issue corresponding prospective injunctive relief requiring RRCA to employ adequate security protocols consistent with legal and industry standards to protect customers' patients' Private Information, including the following:

a. Order RRCA to provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, RRCA must implement and maintain reasonable security measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on RRCA's systems on a periodic basis, and ordering RRCA to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of RRCA's systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

vii. meaningfully educating its customers' patients about the threats they face with regard to the security of their Private Information, as well as the steps they should take to protect themselves.

217. If an injunction is not issued, Plaintiff will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at RRCA. The risk of another such breach is real, immediate, and substantial. If another breach at RRCA occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

218. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to RRCA if an injunction is issued. Plaintiff will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of RRCA's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and RRCA has a pre-existing legal obligation to employ such measures.

219. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at RRCA, thus preventing future injury to Plaintiff and other customers' patients whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class described above, seek the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representatives of the Nationwide Class requested herein;

b. Judgment in favor of Plaintiff and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing RRCA to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members;

e. An order requiring RRCA to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiff and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: November 18, 2024

Respectfully submitted,

/s/ Mason A. Barney
Mason A. Barney (Bar No. 4405809)
Tyler J. Bean (*pro hac vice to be filed)*
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: mbarney@sirillp.com
E: tbean@sirillp.com